

Sep 03, 2020

s/ Jeremy Heacox

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of)
 (Briefly describe the property to be searched)
 or identify the person by name and address))
 Information that is stored at premises)
 controlled by Google concerning 5922)
 Sheridan Rd., Kenosha, WI)

Case No. 20-M-371 (SCD)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____
 (identify the person or describe the property to be searched and give its location):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before 9-17-20 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____
 Hon. Stephen C. Dries
 (United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: 9-3-20, 3:40 pm

City and state: Milwaukee, Wis



Judge's signature

Hon. Stephen C. Dries, U.S. Magistrate Judge

Printed name and title

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

ATTACHMENT A

Property To Be Searched

This warrant is directed to Google LLC and applies to:

- (1) Location History data, sourced from information including GPS data and information about visible wi-fi points and Bluetooth beacons transmitted from devices to Google, reflecting devices that Google calculated were or could have been (as indicated by margin of error, *i.e.*, “maps display radius”) located within the geographical region bounded by the latitudinal and longitudinal coordinates, dates, and times below (“Initial Search Parameters”); and
- (2) identifying information for Google Accounts associated with the responsive Location History data.

Initial Search Parameters

- Date: August 23, 2020
- Time Period: 8:27 PM to 9:45 PM (CST)
- Target Location: Geographical area identified as:
42.580916, -87.821792; 42.580995, -87.821710; 42.581429, -87.821686;
42.581384, -87.822171; 42.580901, -87.822082; 42.580916, -87.821792

Also approximately depicted using the following image:



Google is further ordered to disclose the above information to the Government within 10 days of the issuance of this warrant.

ATTACHMENT B

Particular Items to Be Seized

I. Information to be disclosed by Google

The information described in Attachment A, via the following process:

1. Google shall query location history data based on the Initial Search Parameters specified in Attachment A. For each location point recorded within the Initial Search Parameters, and for each location point recorded outside the Initial Search Parameters where the margin of error (*i.e.*, “maps display radius”) would permit the device to be located within the Initial Search Parameters, Google shall produce to the government information specifying the corresponding unique device ID, timestamp, location coordinates, display radius, and data source, if available (the “Device List”).

2. The government shall review the Device List and identify to Google the devices about which it seeks to obtain Google account identifier and basic subscriber information. The government may, at its discretion, identify a subset of the devices.

3. Google shall disclose to the government identifying information, as defined in 18 U.S.C. § 2703(c)(2), for the Google Accounts associated with each device ID appearing on the Device List about which the government inquires.

II. Information to Be Seized

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 844(i) (arson), involving unknown persons.

Sep 03, 2020

s/ Jeremy Heacox

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the
Eastern District of WisconsinIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No. 20-M-371 (SCD)

Information that is stored at premises controlled by
Google concerning 5922 Sheridan Rd., Kenosha, WI

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the _____ District of _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
Title 18, United States Code, Arson
Section 844

Offense Description

The application is based on these facts:
See the attached affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

RYAN ARNOLD
Digitally signed by RYAN ARNOLD
Date: 2020.09.03 11:25:12 -05'00'

Applicant's signature

ATF SA Ryan Arnold

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ (specify reliable electronic means).

Date: 9-3-20

City and state: Milwaukee, Wis

Hon. Stephen C. Dries, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WISCONSIN

IN THE MATTER OF THE SEARCH OF
INFORMATION THAT IS STORED AT
PREMISES CONTROLLED BY GOOGLE
CONCERNING 5922 SHERIDAN ROAD,
KENOSHA, WI

FILED UNDER SEAL

Case No. **20-M-371 (SCD)**

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Ryan Arnold, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a warrant to search information that is stored at premises controlled by Google, an electronic communication service and remote computing service provider headquartered in Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a warrant under 18 U.S.C. § 2703(c)(1)(A) to require Google to disclose to the government the information further described in Attachment B.I. The government will then review that information and seize the information that is further described in Attachment B.II.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and have been since April 2015. As an ATF Special Agent, I have participated in numerous investigations regarding the unlawful possession of firearms by convicted felons. I have also conducted investigations related to the unlawful use of firearms, firearms trafficking, drug trafficking, and arson. Prior to my employment with ATF, I was a Special Agent with the United States Secret Service (USSS) for nearly 5 years. My duties included providing and planning dignitary protection, drafting and executing federal search

warrants, investigations of organized crime networks, investigations of threats against USSS protectees, fraud networks, counterfeit currency investigations, and other financial crime investigations. Before my tenure with the USSS, I served as a police officer with the Chicago Police Department (CPD). During part of my career as a CPD Officer, I was assigned to the Organized Crime Division-Gang Enforcement Unit. My responsibilities included the investigations of street gangs, narcotics distribution, firearms violations, robbery, home invasions, operating in an undercover capacity, and the authoring and execution of search warrants.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 844(i) (arson) have been committed by unknown persons. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. Specifically, the United States District Court for the Eastern District of Wisconsin is “a district court of the United States that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND RELATING TO GOOGLE AND RELEVANT TECHNOLOGY

6. Based on my training and experience, I know that cellular devices, such as mobile telephone(s), are wireless devices that enable their users to send or receive wire and/or electronic

communications using the networks provided by cellular service providers. Using cellular networks, users of many cellular devices can send and receive communications over the Internet.

7. I also know that many devices, including but not limited to cellular devices, have the ability to connect to wireless Internet (“wi-fi”) access points if the user enables wi-fi connectivity. These devices can, in such cases, enable their users to send or receive wire and/or electronic communications via the wi-fi network. A tablet such as an iPad is an example of a device that may not have cellular service but that could connect to the Internet via wi-fi. Wi-fi access points, such as those created through the use of a router and offered in places like homes, hotels, airports, and coffee shops, are identified by a service set identifier (“SSID”) that functions as the name of the wi-fi network. In general, devices with wi-fi capability routinely scan their environment to determine what wi-fi access points are within range and will display the names of networks within range under the device’s wi-fi settings.

8. Based on my training and experience, I also know that many devices, including many cellular and mobile devices, feature Bluetooth functionality. Bluetooth allows for short-range wireless connections between devices, such as between a device such as a cellular phone or tablet and Bluetooth-enabled headphones. Bluetooth uses radio waves to allow the devices to exchange information. When Bluetooth is enabled, a device routinely scans its environment to identify Bluetooth devices, which emit beacons that can be detected by devices within the Bluetooth device’s transmission range, to which it might connect.

9. Based on my training and experience, I also know that many cellular devices, such as mobile telephones, include global positioning system (“GPS”) technology. Using this technology, the device can determine its precise geographical coordinates. If permitted by the user, this information is often used by apps installed on a device as part of the apps’ operation.

10. Based on my training and experience, I know Google is a company that, among other things, offers an operating system (“OS”) for mobile devices, including cellular phones, known as Android. Nearly every device using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.

11. In addition, based on my training and experience, I know that Google offers numerous apps and online-based services, including messaging and calling (*e.g.*, Gmail, Hangouts, Duo, Voice), navigation (Maps), search engine (Google Search), and file creation, storage, and sharing (*e.g.*, Drive, Keep, Photos, and YouTube). Many of these services are accessible only to users who have signed in to their Google accounts. An individual can obtain a Google account by registering with Google, and the account identifier typically is in the form of a Gmail address (*e.g.*, example@gmail.com). Other services, such as Maps and YouTube, can be used with limited functionality without the user being signed in to a Google account.

12. Based on my training and experience, I also know Google offers an Internet browser known as Chrome that can be used on both computers and mobile devices. A user has the ability to sign-in to a Google account while using Chrome, which allows the user’s bookmarks, browsing history, and other settings to be uploaded to Google and then synced across the various devices on which the subscriber may use the Chrome browsing software, although Chrome can also be used without signing into a Google account. Chrome is not limited to mobile devices running the Android operating system and can also be installed and used on Apple devices and Windows computers, among others.

13. Based on my training and experience, I know that, in the context of mobile devices, Google’s cloud-based services can be accessed either via the device’s Internet browser

or via apps offered by Google that have been downloaded onto the device. Google apps exist for, and can be downloaded to, devices that do not run the Android operating system, such as Apple devices.

14. According to my training and experience, as well as open-source materials published by Google, I know that Google offers accountholders a service called “Location History,” which authorizes Google, when certain prerequisites are satisfied, to collect and retain a record of the locations where Google calculated a device to be based on information transmitted to Google by the device. That Location History is stored on Google servers, and it is associated with the Google account that is associated with the device. Each accountholder may view their Location History and may delete all or part of it at any time.

15. Based on my training and experience, I know that the location information collected by Google and stored within an account’s Location History is derived from sources including GPS data and information about the wi-fi access points and Bluetooth beacons within range of the device. Google uses this information to calculate the device’s estimated latitude and longitude, which varies in its accuracy depending on the source of the data. Google records the margin of error for its calculation as to the location of a device as a meter radius, referred to by Google as a “maps display radius,” for each latitude and longitude point.

16. Based on open-source materials published by Google and my training and experience, I know that Location History is not turned on by default. A Google accountholder must opt-in to Location History and must enable location reporting with respect to each specific device and application on which they use their Google account in order for that usage to be recorded in Location History. A Google accountholder can also prevent additional Location History records from being created at any time by turning off the Location History setting for

their Google account or by disabling location reporting for a particular device or Google application. When Location History is enabled, however, Google collects and retains location data for each device with Location Services enabled, associates it with the relevant Google account, and then uses this information for various purposes, including to tailor search results based on the user's location, to determine the user's location when Google Maps is used, and to provide location-based advertising. As noted above, the Google accountholder also has the ability to view and, if desired, delete some or all Location History entries at any time by logging into their Google account or by enabling auto-deletion of their Location History records older than a set number of months.

17. Location data, such as the location data in the possession of Google in the form of its users' Location Histories, can assist in a criminal investigation in various ways. As relevant here, I know based on my training and experience that Google has the ability to determine, based on location data collected and retained via the use of Google products as described above, devices that were likely in a particular geographic area during a particular time frame and to determine which Google account(s) those devices are associated with. Among other things, this information can indicate that a Google accountholder was near a given location at a time relevant to the criminal investigation by showing that his/her device reported being there.

18. Based on my training and experience, I know that when individuals register with Google for an account, Google asks subscribers to provide certain personal identifying information. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because

the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, this information often provide clues to their identity, location, or illicit activities.

19. Based on my training and experience, I also know that Google typically retains and can provide certain transactional information about the creation and use of each account on its system. This information can include the date on which the account was created, the length of service, records of login (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, Google often has records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

PROBABLE CAUSE

20. On August 23, 2020, Mr. Jacob Blake was shot multiple times by personnel of the Kenosha Police Department. That incident precipitated both non-violent protests and violent rioting, the latter of which included various arsons throughout the city of Kenosha, Wisconsin. The unrest and violence grew so dangerous that the Wisconsin National Guard eventually deployed over 1,000 individuals to the area, in an effort to keep the peace. Federal resources were also marshalled to investigate various crimes associated with these incidents, including arsons and looting. The ATF, for its part, deployed its National Response Team of 50 expert arson investigators to Kenosha, who are currently processing scenes, collecting video evidence,

and identifying potential subjects. The instant warrant application is made as part of that response effort.

21. Gulf-Lakeside Fuels, located at 5922 Sheridan Road, Kenosha, Wisconsin, was broken into and looted the evening of August 23, 2020. As part of the investigation into that crime and related nearby arsons, law enforcement obtained and reviewed video surveillance footage generated by the proprietors of Gulf-Lakeside Fuels.

22. That video showed numerous, currently unknown, individuals entering Gulf-Lakeside Fuels and stealing materials frequently used by arsonists.

23. At approximately 8:30 PM, the video surveillance depicts an unknown male break the window of the front door to gain entry to the business. Between 8:30 PM and 8:53 PM, the video surveillance depicts dozens of subjects entering the store and looting.

24. At approximately 9:18 PM, the video surveillance again shows subjects entering the store and looting. A review of the video suggests at least ten people enter the store (some may have been the same subjects who previously entered). At approximately 9:21 PM, the video surveillance depicts a white male (wearing jeans, a hat and a black t-shirt, with a tattoo on his forearm) entering the business with a clear plastic bag. This same subject begins filling his plastic bag with multiple white bottles that I believe, based on my training and experience and the depiction of these bottles, contained charcoal lighter fluid. At 8:22 PM, the subject exits the store. Around that time, multiple bottles of lighter fluid fall out of the subject's bag just outside front door. I know, from training and experience, that lighter fluid is commonly used in arsons; more specifically, I know that ignitable fluids, such as lighter fluid, are frequently stolen — and used— during arsons perpetuated during civil unrest of the sort experienced recently in Kenosha.

25. At approximately 8:32 PM, video surveillance footage depicts a black female (wearing pants with “Just Do It” written on the leg) taking a bottle of charcoal lighter fluid. She exits the store about 12 seconds after entering.

26. Looting activity ceased at this location at approximately 9:35 when Kenosha Police Department (KPD) officers arrived and arrested two subjects.

27. After the looting of Gulf-Lakeside Fuels, numerous businesses in close proximity were targets of arson. To illustrate, a list of 911 calls to KPD and the Kenosha Fire Department (KPD) follows:

- 11:35 PM (8/23/2020): Structure fire call at 1112 56th Street (approximately .4 miles from Gulf-Lakeside Fuels, where lighter fluid was stolen);
- 12:07 AM (8/24/2020): Structure fire call at 912 56th Street (approximately .3 miles from Gulf-Lakeside Fuels, where lighter fluid was stolen);
- 12:20 AM (8/24/2020): Another structure fire call at 912 56th Street (approximately .3 miles from Gulf-Lakeside Fuels, where lighter fluid was stolen);
- 12:51 AM (8/24/2020): Fire call at 5608 10th Avenue (approximately .3 miles from Gulf-Lakeside Fuels, where lighter fluid was stolen);
- 2:23 AM (8/24/2020): Fire call at 5810 8th Avenue (approximately .3 miles from Gulf-Lakeside Fuels, where lighter fluid was stolen);
- 3:02 AM (8/24/2020): Fire call at 5716 6th Street (approximately .3 miles from Gulf-Lakeside Fuels, where lighter fluid was stolen);

28. I am further aware of at least one other occasion where it is likely that lighter fluid, packaged in a white bottle similar in appearance to the lighter fluid stolen from Gulf-Lakeside Fuels, was used during the civil unrest to ignite a fire. I have reviewed video footage dated August 25, 2020, which shows, from approximately 11:42 PM to 11:48 PM, an unknown black subject (wearing a white t-shirt, white face covering, and black jeans) holding a white bottle that appeared, based on my training and experience, to contain lighter fluid. The subject sprayed the contents of this bottle into a burning vehicle located at 6226 Sheridan Road, Kenosha, Wisconsin. This is the location of “Car Source” vehicle repairs, which is engaged in interstate commerce.

29. On August 31, 2020, I spoke with the owner of Gulf-Lakeside Fuels, who confirmed to me that: (i) his store stocked various forms of lighter fluid and (ii) the lighter fluid bottle as described above from the August 25 incident matched the description of one sort of lighter fluid provided at Gulf-Lakeside Fuels.

30. Given: (i) the looting and theft of various bottles of lighter fluid from Gulf-Lakeside Fuels; (ii) the subsequent series of fires in close proximity to that theft; (iii) my knowledge regarding the frequent theft and use of lighter fluid during periods of civil unrest; and (iv) the similarity between the lighter fluid stolen from Gulf-Lakeside Fuels and the lighter fluid used during the arson at 6226 Sheridan Road, I submit that there is probable cause to search information that is currently in the possession of Google and that relates to the devices that reported being within the Target Location described in Attachment A during the time period described in Attachment A for evidence of the crimes under investigation. The information to be searched includes (1) identifiers of each device; (2) the location(s) reported by each device to

Google and the associated timestamp; and (3) basic subscriber information for the Google account(s) associated with each device.

31. The proposed warrant sets forth a multi-step process whereby the government will obtain the information described above. Specifically, as described in Attachment B.I:

- a. Using Location History data, Google will identify those devices that it calculated were or could have been (based on the associated margin of error for the estimated latitude/longitude point) within the Target Location described in Attachment A during the time period described in Attachment A. For each device, Google will provide a anonymized identifier, known as a Reverse Location Obfuscation Identifier (“RLOI”), that Google creates and assigns to device for purposes of responding to this search warrant; Google will also provide each device’s location coordinates along with the associated timestamp(s), margin(s) of error for the coordinates (*i.e.*, “maps display radius”), and source(s) from which the location data was derived (*e.g.*, GPS, wi-fi, bluetooth), if available. Google will not, in this step, provide the Google account identifiers (*e.g.*, example@gmail.com) associated with the devices or basic subscriber information for those accounts to the government.
- b. The government will identify to Google the devices appearing on the list produced in step 1 for which it seeks the Google account identifier and basic subscriber information. The government may, at its discretion, identify a subset of the devices.

c. Google will then disclose to the government the Google account identifier associated with the devices identified by the government, along with basic subscriber information for those accounts.

32. This process furthers efficiency and privacy by allowing for the possibility that the government, upon reviewing contextual information for all devices identified by Google, may be able to determine that one or more devices associated with a Google account (and the associated basic subscriber information) are likely to be of heightened evidentiary value and warrant further investigation before the records of other accounts in use in the area are disclosed to the government.

CONCLUSION

33. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c).

34. I further request that the Court direct Google to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property To Be Searched

This warrant is directed to Google LLC and applies to:

- (1) Location History data, sourced from information including GPS data and information about visible wi-fi points and Bluetooth beacons transmitted from devices to Google, reflecting devices that Google calculated were or could have been (as indicated by margin of error, *i.e.*, “maps display radius”) located within the geographical region bounded by the latitudinal and longitudinal coordinates, dates, and times below (“Initial Search Parameters”); and
- (2) identifying information for Google Accounts associated with the responsive Location History data.

Initial Search Parameters

- Date: August 23, 2020
- Time Period: 8:27 PM to 9:45 PM (CST)
- Target Location: Geographical area identified as:
42.580916, -87.821792; 42.580995, -87.821710; 42.581429, -87.821686;
42.581384, -87.822171; 42.580901, -87.822082; 42.580916, -87.821792

Also approximately depicted using the following image:



Google is further ordered to disclose the above information to the Government within 10 days of the issuance of this warrant.

ATTACHMENT B

Particular Items to Be Seized

I. Information to be disclosed by Google

The information described in Attachment A, via the following process:

1. Google shall query location history data based on the Initial Search Parameters specified in Attachment A. For each location point recorded within the Initial Search Parameters, and for each location point recorded outside the Initial Search Parameters where the margin of error (*i.e.*, “maps display radius”) would permit the device to be located within the Initial Search Parameters, Google shall produce to the government information specifying the corresponding unique device ID, timestamp, location coordinates, display radius, and data source, if available (the “Device List”).

2. The government shall review the Device List and identify to Google the devices about which it seeks to obtain Google account identifier and basic subscriber information. The government may, at its discretion, identify a subset of the devices.

3. Google shall disclose to the government identifying information, as defined in 18 U.S.C. § 2703(c)(2), for the Google Accounts associated with each device ID appearing on the Device List about which the government inquires.

II. Information to Be Seized

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 844(i) (arson), involving unknown persons.